FedizProposal

Fediz - Federation based Web SSO

Abstract

The idea of WS-Federation for Web SSO is to externalize the authentication process to a centralized authentication server (called Identity Provider (IDP)) which can support any kind of authentication mechanism. The IDP issues a security token like SAML which contains the authenticated entity as well as role information and/or other claim data of a user like name, email, others which is sent to the application (called Relying Party (RP)).

Use case for an application: Usually, fine graind authorization is not directly dependent on the authenticated user. Instead, the user is required to get some user attributes from an identity system (LDAP, whatever). You implement authorization based on these attributes. In WS-Federation, these claim attributes are added to the SAML token (standardized too) and the application has the possibility to tell the IDP what kind of claims the need (HTTP parameter or WS-Federation metadata document)

Background

The Federation based Web SSO design based on the OASIS WS-Federation spec is described in the following blog:

http://owulff.blogspot.com/2011/10/configure-and-deploy-identity-provider.html

Rationale

Fediz federation will enable you to integrate new businesses for your existing business assets very quickly without touching the applications at all. It's also a cloud enabler for web applications.

Current Status

Fediz code base has been created for a specific customer.

Open Source

Since the beginning, Fediz is an Open Source project using the Apache license.

Known Risks

Orphaned Products

Fediz is already deployed in production for a customer. Fediz is getting traction with developers and thus the risks of it being orphaned are minimal.

Inexperience with Open Source

Most of the Fediz committers are Apache committers, on several Apache projects.

Homogeneous Developers

The initial set of committers is from a small set of organizations. However, we expect that once approved for incubation, the project will attract new contributors from diverse organizations and will thus grow organically. The participation of developers from several different organizations in the mailing list is a strong indication for this assertion.

Reliance on Salaried Developers

It is expected that Fediz will be developed on salaried and volunteer time, although all of the initial developers will work on it mainly on salaried time.

Relationships with Other Apache Products

Fediz uses services provided by Apache CXF.

A Fascination with the Apache Brand

The reason for joining Apache is to foster a healthy community of contributors and consumers around the project. This is facilitated by ASF and that is the primary reason we would like Fediz to become an Apache project.

Source and Intellectual Property Submission Plan

The initial source is Apache 1.0 licensed. An IP Clearance is in progress to update to Apache 2.0.

External Dependencies

Fediz doesn't depend to non-Apache project.

Cryptography

Fediz does not depend upon any cryptography tools or libraries.

Required Resources

Mailing lists

- fediz-private (with moderated subscriptions)
- fediz-dev
- fediz-commits
- fediz-user

Subversion Directory

https://svn.apache.org/repos/asf/incubator/fediz

Issue Tracking

JIRA Fediz (FEDIZ)

Other Resources

The existing code already has unit and integration tests so we would like a Jenkins instance to run them whenever a new patch is submitted. This can be added after project creation.

Initial Committer

- Oliver Wulff (owulff@talend.com)
- Olivier Lamy (olamy@apache.org)
- Jean-Baptiste Onofré (jbonofre@apache.org)
- Jürg Portmann (juerg.portmann@noveit.ch)
- Colm O'hEigeartaigh (coheigea@apache.org)

Affiliations

- Oliver Wulff, Talend
- Jean-Baptiste Onofré, Talend
- Olivier Lamy, Talend
- Colm O'hEigeartaigh, Talend

Sponsors

Champion

- Jean-Baptiste Onofré (jbonofre@apache.org)

Nominated Mentors

- Jean-Baptiste Onofré (jbonofre@apache.org)
- Olivier Lamy (olamy@apache.org)
- Mohammad Nour (mnour@apache.org)